

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION**

UNITED STATES OF AMERICA

v.

Case No. 8:19-cr-68-T-24TGW

RICHARD FRANKLIN JENSEN, III,

Defendant.

_____ /

ORDER

THIS CAUSE comes before the Court on Defendant Richard Franklin Jensen's Motion to Suppress Evidence (Doc. 27) and the Government's Response in Opposition with supporting exhibits (Doc. 32). The Court, having carefully reviewed the parties' submissions and having now conducted a hearing on the matter on July 23, 2019, finds that the Motion must be denied for the reasons explained below.

I. Background

On February 20, 2019, a grand jury indicted Defendant, Richard F. Jensen III, for knowingly attempting to persuade, induce, entice, and coerce a minor in sexual activity in violation of 18 U.S.C. § 2422(b), and knowingly attempting to transfer obscene matter to a minor in violation of 18 U.S.C. § 1470. On March 7, 2016, a magistrate judge in the Northern District of Georgia issued a search warrant for the Defendant's residence, located at 625 Channing Drive

N.W., Atlanta, Georgia 30318. (Doc. 32, Ex. A (Application and Search Warrant, case number 1:16-MC-0198). On March 8, 2016, the search warrant was executed at Defendant's residence. The alleged criminal acts that are the basis for the search warrant occurred from May 23, 2015 through June 4, 2015. This included emails and text messages with an undercover agent, Homeland Security Investigations Special Agent Terri Botterbusch, posing as a fictitious mother and twelve year old daughter.

Defendant was not at the residence when law enforcement officers arrived to execute the search warrant. Defendant arrived after law enforcement arrived on scene to execute the search warrant. Once he arrived, law enforcement instructed him to exit his vehicle, and he complied. Defendant immediately stated that he wanted an attorney. Defendant was searched for weapons and his cell phone, an Apple iPhone 6 Plus, was removed from his person.

Defendant asked Special Agent Diana Ford ("SA Ford") if he could use his phone to call his attorney. The attorney's cell phone number was stored in Defendant's phone. Defendant was only allowed to call his attorney via his cell phone after providing his password to SA Ford to unlock his phone.

II. Defendant's Motion

Defendant moves the Court, pursuant to Rule 12(b)(3)(c) and the Fourth, Fifth and Sixth Amendments, to suppress the evidence and data from any computer or device searched in whole or in part via a password derived from the illegal search of the iPhone 6 Plus. Defendant argues that the search was illegal because when law enforcement asked for his cell phone password after he invoked his right to an attorney they violated his Fifth Amendment right to silence. Further, because the situation had become adversarial for Defendant and law enforcement had availed themselves of the judicial process to get the search warrant of the residence, Defendant's Sixth

Amendment right to counsel had already attached.

Defendant also asserts that had he not provided his cell phone password, law enforcement would not have been able to unlock the phone and ultimately gain access to Defendant's iCloud account and all of his passwords for other devices and accounts which had been stored for safekeeping on the iPhone 6 Plus. Many electronic devices were seized from Defendant's residence including an iPhone 5, iMac desktop computer, and an Apple MacBook Pro Laptop computer, which was password protected and encrypted. Defendant argues that any evidence derived from his iPhone 6 Plus, including passwords for his laptop, should be determined to be fruit of the poisonous tree under the exclusionary rule, which bars admission of evidence obtained in violation of the Constitution including evidence derived from the illegal conduct, as well as other incriminating evidence derived from the primary evidence.

Finally, Defendant moves to suppress all evidence obtained via the search of his residence, on grounds that the search warrant lacked probable cause because it was based on stale (nine months' old) information.

III. Discussion

A. Mootness as to Defendant's Fifth and Sixth Amendment and Fruit of the Poisonous Tree Arguments

The Government stated that it does not intend to introduce or rely on any evidence extracted from the defendant's Apple iPhone 6 Plus. The Government intends to instead rely on evidence extracted from the iPhone 5 found in Defendant's residence when the search warrant was executed. Computer Forensic Analyst James Stone ("CFA Stone") testified at the hearing that he mailed the iPhone 5 to Cellebrite Advanced Investigative Services ("Cellebrite") for the purpose of unlocking the device and that on November 7, 2016, Cellebrite returned the iPhone 5

after extracting the password using Cellebrite software. CFA Stone then used the password that was provided by Cellebrite (and not any information gained from Defendant's iPhone 6 Plus) to unlock Defendant's iPhone 5 and successfully extract data from the device.

The Government also intends to rely on evidence extracted from the iMac desktop computer found in Defendant's residence when the search warrant was executed. CFA Stone testified at the hearing that there was no encryption on the iMac desktop and that the device was not accessed using a password (or any information gained from Defendant's iPhone 6 Plus), but rather, he took a forensic image of the computer in order to view and analyze its contents.

In light of the foregoing, Defendant's Motion to Suppress pertaining to his Fifth and Sixth Amendment rights and his fruit of the poisonous tree argument, as to the iPhone 6 Plus that was seized from his person and the iPhone 5 and iMac desktop seized from the residence are denied. As to the Apple MacBook Pro laptop seized from the residence, the Government states that it has not been able to access the device because it is encrypted, but does it not waive the right to rely on any evidence contained on the laptop should they be able to access it in the future.

B. Staleness

Defendant argues that the probable cause set forth in the search warrant affidavit was stale and, therefore, in violation of his Fourth Amendment right to be free from unreasonable searches and seizures. Nine months lapsed between the end of the criminal activity charged against Defendant in the indictment (June 4, 2015) and the execution of the search warrant (March 8, 2016). Defendant argues that law enforcement should have sought a search warrant expeditiously since Defendant suspected he was the target of a federal criminal investigation on June 4, 2015, and could have destroyed any evidence of criminal activity directly related to his interactions with the fictitious mother and daughter and any other potential crimes including child pornography.

Therefore, there was not probable cause to believe Defendant's residence would contain evidence of criminal activity nine months later.

To satisfy the staleness doctrine, probable cause must exist and be demonstrated by supporting information at the time a warrant is issued. *U.S. v. Bervaldi*, 226 F.3d 1256, 1264 (11th Cir. 2000); *see also*, *U.S. v. Harris*, 20 F.3d 445, 450 (11th Cir.1994). For probable cause to exist, the information used to obtain a search warrant must be timely. *Harris*, 20 F.3d at 450. However, there is "no particular rule or time limit for when information becomes stale." *Id.* The staleness of an issue must be decided by evaluating the facts of a particular case. *Bervaldi*, 226 F.3d at 1265 (quoting *U.S. v. Hyde*, 574 F.2d 856, 865 (5th Cir.1978)). In addition to the length of time, courts also consider the "nature of the suspected crime (discrete crimes or ongoing conspiracy), habits of the accused, character of the items sought, and nature and function of the premises to be searched." *Id.* at 1265; *Harris*, 20 F.3d at 450. Timeliness is of less significance if the alleged conduct is of a protracted and continuous nature. *Id.* at 1265 (quoting *Bastida v. Henderson*, 487 F.2d 860, 864 (5th Cir.1973)). Probable cause may be derived from a "particularized and objective basis" for suspicion of wrong doing by an officer based on his or her "experience and specialized training." *U.S. v. Arvizu*, 534 U.S. 266, 273 (2002).

In *U.S. v. Kirkham*, the court denied the defendant's motion to suppress because the affidavit in support of the search warrant was determined not to be stale, even though it was issued **six months** after communication between the defendant and victim ended. 719 F. App'x 994 (11th Cir. 2018) (unpublished) (emphasis added). The *Kirkman* defendant was convicted for enticement of a minor under 18 U.S.C. § 2442(b) and possession of child pornography under 18 U.S.C. § 2252A(a)(5)(B). *Id.* Probable cause from a six month old affidavit was not deemed to be stale because it was not "entirely unreasonable" for officers to believe Kirkham still possessed

communications and explicit photos of the minor. *Id.* Further, the court held that the “good-faith exception” prevented the suppression of evidence obtained by law enforcement. *Id.* at 995 (citing *U.S. v. Leon*, 468 U.S. 897, 913 (1984)). The “good-faith exception” prevents the suppression of “reliable physical evidence seized by officers reasonably relying on a warrant issued by a detached and neutral magistrate.” *Leon*, 468 U.S. 897, 913 (1984).

The mere passage of time is unlikely to render information in a child exploitation warrant stale because child exploitation evidence has a long preservation period, is not transient or easily degraded by the passage of time, and is forensically recoverable even in the case of file corruption, deletion, or steganography. *See United States v. Mathis*, No. 8:12-cr-457-T-30MAP, 2013 WL 869511 (M.D. Fla. Feb. 19, 2013). In *Mathis*, the court denied the defendant’s motion to suppress evidence seized from a cellphone based on staleness and recklessly misleading information. *Id.*¹ The magistrate judge explained in his report and recommendation that although there was a **six-year delay**, “digital files are qualitatively different” and forensic examiners can usually recover deleted digital files, and child pornography collectors are unlikely to dispose of images. *Id.* at *6 (emphasis added). *See also United States v. Lovvorn*, 524 F. App’x 485, 487 (11th Cir. 2013) (denying motion to suppress based on staleness where information presented to the state judge was no more than nine to twelve months old) (quoting *United States v. Sarras*, 575 F.3d 1191, 1197, 1203 (11th Cir.2009);

Here, the passage of nine months did not alter the sufficiency of the probable cause to search Defendant’s residence and, thus, the search warrant was not stale. Defendant’s conduct

¹ The report and recommendation of the magistrate judge to deny the motion to suppress was adopted, confirmed, and approved in all respects by the district judge. *United States v. Mathis*, No. 8:12-cr-457-30MAP, 2013 WL 868250 (M.D. Fla. Mar. 7, 2013).

and conversations with Agent Botterbusch suggest that his crimes were continuous and protracted. For example, using the username “Hotdirtystud” on “Motherless.com,” Defendant stated in his profile that “[he] would love to find another new sub to train and use regularly, especially since [his] last graduated from school and moved away.” (Doc. 32-1, pp. 15-16). On May 28, 2015, Defendant stated in an email to Agent Botterbusch, “I never have been and never would be rough with a little one.” (*Id.* at p.10). On May 30, 2015, Defendant stated the following in an email addressed to Agent Botterbusch: “I have actually taught two different younger girls about sex and trained them in the art of pleasing a man. Both of them started with me when they were a little bit older than your [Agent Botterbusch’s] daughter and we had great experiences and relationships that lasted several years.” (*Id.* at p. 13). Lastly, on June 4, 2015, Defendant stated in an email, “I mean you’re asking me to do something very illegal. I am happy & willing to do it, but I just have to ask questions to make sure it’s safe for me.” (*Id.* at p. 21). These communications suggest that Defendant may have previously sent similar communications or even previously engaged in sexual conduct with minors before responding to Agent Botterbusch’s online advertisement. They also suggest that Defendant’s crimes may have occurred over several years and, thus, it was reasonable to believe that Defendant may continue to engage in this type of behavior.

Additionally, probable cause existed after nine months because of the character of the items sought in the search warrant, including computers, computer peripherals, and electronic media storage devices. Law enforcement sought records and documents in the format of e-mail messages, chat logs, and other electronic messages pertaining Jensen’s alleged criminal conduct. (Doc. 32-1, Ex. A, Att. B ¶ 5). Agent Botterbusch established in the search warrant affidavit that based on her training and experience, child pornography was likely to be at Defendant’s residence at the time of the search. (*See* Doc. 32-1, ¶¶ 8(h) – (j), 39). She further explained that electronic

communications can be saved or stored on the computer intentionally and unintentionally. (*Id.* at ¶ 8(h)). Moreover, a computer user's internet activities generally leave traces or footprints in the web cache and history files of the web browser and is often maintained indefinitely until overwritten by other data. (*Id.*) Based on Agent Botterbusch's years of training and experience, she stated she knew that computer files or remnants of such files can be recovered months or even years after they have been initially downloaded, viewed, or deleted. Exhibit A ¶ 39. Although Defendant argues that he could have physically destroyed any of his electronic devices, leaving the digital files on them unrecoverable, it is unlikely that Defendant would destroy his expensive electronic devices, rather than make efforts to delete or hide the digital files on those devices. Thus, it was reasonable to believe that the items being sought by law enforcement would still be in the residence when the warrant issued.

Finally, the "good-faith exception" to suppression of the evidence obtained by law enforcement, as set forth in *United States v. Leon*, 468 U.S. 897, 913 (1984), applies here. The exception prevents the suppression of reliable physical evidence seized by officers reasonably relying on a warrant issued by a detached and neutral magistrate. There is no reason to believe that the magistrate judge who issued the search warrant for Defendant's residence, knowing that there had been a nine month delay, was anything but neutral and detached, and therefore, law enforcement had a good faith belief that they could rely on her decision. Although Defendant urges that the magistrate judge could not have remained neutral and detached after reading the explicit and scandalous details of the investigation set forth in the search warrant affidavit, the facts set forth by Agent Botterbusch, including the content of the emails, were necessary in order to demonstrate violations by Defendant of 18 U.S.C. §§ 2422(b) and 1470 and to establish probable cause for the search warrant. There is no basis for Defendant's argument that the

magistrate judge was not neutral and detached.

ACCORDINGLY, it is **ORDERED AND ADJUDGED**:

Defendant Richard Franklin Jensen's Motion to Suppress Evidence (Doc. 27) is **DENIED**.

DONE AND ORDERED at Tampa, Florida, this 25th day of July, 2018.


SUSAN C. BUCKLEW
United States District Judge

Copies to:
Counsel of Record